UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/446,525	12/27/1999	MASAYUKI KANDA	162/540	2460

7590 08/13/2003

POLLOCK VANDE SANDE & PRIDDY
PO BOX 19088
WASHINGTON, DC 20036-3425

EXAMINER
VAUGHAN, MICHAEL R

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/13/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/446,525	KANDA ET AL.	
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *14-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *14-30,32-34,36-44 and 46-49* is/are rejected.

7)☒ Claim(s) *31,35, and 45* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *4* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

Detailed Action

Claims 14-49 have been examined.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on December 27, 1999 was filed. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Claim Objections

Claim 17 is objected to because of the following informalities: typographic error: "don" – on--. Appropriate correction is required.

Claim 39 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 39 is the same as its parent claim 35. It clearly does not further limit claim 35.

Claims 31, 35, and 45, are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 49 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. There is some difference between this claim and the information specified in the disclosure. The second exclusive-OR circuit is not mentioned but is referred to on page 16, line 6 (lacks antecedent basis). The first exclusive-OR circuit doesn't accurately describe the manner in which the data subjected as cited in the specification.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 14-27, 40, and are rejected under 35 U.S.C. 103(a) as being unpatentable over DES (Data Encryption Standard, National Bureau of Standards (U.S.), in view of Matsui (New Block Encryption Algorithm MISTY).

As per claim 14, DES teaches:

initial splitting of data (FIG. 1);

Key storage (inherent) (FIG. 1);

Plurality of rounds cascaded together (FIG. 1);

Final combining part (inverse initial permutation) (FIG. 1);

Non-linear function (f) (FIG. 1);

Linear operation part (XOR) (FIG. 1);

Swapping part (FIG. 1);

Key-dependent linear transformation part within the nonlinear function (FIG. 2);

Splitting part (FIG. 2);

Plurality of first nonlinear transformation parts (FIG. 2)

First linear transformation part (FIG. 2);

Combining part (p) (FIG. 2).

DES is silent in disclosing a second nonlinear transformation part. Mitsui teaches a plurality of nonlinear parts to operate on data. Mitsui teaches that within each round of ciphering, the data passes through S-boxes (nonlinear transformation parts) more than once (FIG. 4). Linear transformations occur between S-boxes. Mitsui teaches that computation is faster when the size of the data is small (page 1). It is notoriously well known in the art that the strength of DES like algorithms rely on the nonlinear transformations. Therefore, it is obvious that there need to be many nonlinear transformations. MISTY, as taught by Mitsui has increased the number of nonlinear transformation by subjecting the data to several sets of S-boxes in each round. In view of this, it would have been obvious to one of ordinary skill in the art to use two sets of nonlinear transformation within each round of a DES like algorithm.

As per claim 15, DES teaches the use of keys in a linear transformation prior to going into the S-boxes on a plurality of routes (FIG 2).

As per claims 16, 17, 19, and 20, DES teaches that a linear transformation using the secret key is performed in each round (FIG 2). DES performs this function at the start of the nonlinear function. Performing the exact same linear function again at the end of the nonlinear function does not constitute a novel difference. DES teaches the linear function and using it twice in the same round does not part from the scope of the prior art.

As per claims 18 and 21, DES teaches linearly combining the key and the data (FIG 2). It is notoriously well known in the art that XOR'ing is function to linearly combine bits. Therefore it is inherent that the data can be XOR'ed with the key, bit by bit.

As per claims 22, 23, 24, 25, 26, 27 and 40, and 41, the scope of DES teaches the use of performing a linear transformation to the input data and a secret key. Using an additional initial and final linear transformation functions does not constitute a novel difference.

Claim 28, 29, 30, 32, 33, 34, 36, 37, 38, 42, 43, 44, 46, 47, and 48 rejected under 35 U.S.C. 103(a) as being unpatentable over DES and Mitsui as applied to claims 14, 22, 23, 24, 25, 26, and 40 above, and further in view of Kwan (The Design of the ICE Encryption Algorithm).

As per claims 28, 29, 32, 33, 36, 37, 42, 43, 46, and 47, the combined teachings of DES and Matsui are silent in disclosing that there are explicitly four routes. The combination of Matsui's recursive S-box structure into the DES algorithm makes having multiple S-boxes functions obvious within each round. The teaching of Kwan discloses, in his ICE algorithm, that he breaks the data into four parts, which traverse down four paths (FIG. 2). Each path leads to a nonlinear S-box. Kwan chooses to break down the data into four pieces contrary to Matsui's two pieces. Both authors break down the chunks whereby the calculations can be performed efficiently within the resources of the device. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to have four routes leading to the nonlinear transformation devices.

As per claims 30, 34, 38, 44, and 48, the combined teachings of DES and Matsui are silent in disclosing that in the first and fourth routes lead to a second nonlinear transformation. The examiner sites the same rationale for motivation as recited in the rejection of claims 28, 29, 32, 33, 36, 37, 42, 43, 46, and 47. The motivation behind having more than one nonlinear transformation in each round is to increase the strength of the algorithm in a fewer number of rounds. These additional computations require more time and resources. It is well known in the art that DES like algorithms base their strength in the nonlinear transformations. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to increase the number of nonlinear transformation by routing some of the data chunks through a second nonlinear transformation. Of the four routes, any number of them could be sent to the second nonlinear transformation. The motivation is to balance the strength of the algorithm within the confines of the resources.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7239 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Michael R Vaughan
Examiner
Art Unit 2131

MV

August 7, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100